5 Must-Have Features for a Modern Threat Protection Solution

Introduction: Why Traditional Tools Fall Short

Today's adversaries are faster, more adaptable, and increasingly automated, leveraging AI to scale phishing campaigns, evade detection, and exploit misconfigurations in real time. Yet many enterprises still rely on outdated tools that depend on manual workflows, siloed visibility, and legacy rules.

Modern threat protection requires modernization across technology, process, and expertise.

This checklist outlines the five essential features every organization should have in place to stay protected, and how C1 and Palo Alto Networks work together to deliver them through integrated, AI-powered platforms and expert services.

---

1 Real-Time Detection and Response with AI-Powered Automation

What it is: This refers to the ability to detect, investigate, and contain threats automatically within seconds, not hours or days. AI-driven platforms like Palo Alto's Cortex XSIAM use behavioral analysis and machine learning to detect threats in real time and trigger automated playbooks.

Why it matters: Legacy SIEMs and endpoint solutions often generate high volumes of alerts, most of which are false positives. This overwhelms security teams and delays response to actual threats, increasing risk.

C1 Enhancement: C1's Professional Services team helps design and deploy Palo Alto Networks' real-time detection platforms—such as Cortex XSIAM—ensuring proper integration with your environment and alignment with your threat response goals. While C1 does not offer Managed Services for XSIAM, we can enable automation and response workflows that accelerate detection and reduce manual triage.

☐ Yes ☐ No ☐ Not sure

2 Unified Visibility Across Endpoint, Cloud, and Network

What it is: Unified visibility means your security platform collects, correlates, and analyzes telemetry from all parts of your IT environment, including cloud workloads, SaaS apps, endpoints, and network traffic, in one place.

Why it matters: Attackers exploit gaps between tools and platforms. If your endpoint protection can't talk to your cloud security stack—or your network monitoring lacks context, you'll miss the signs of lateral movement or privilege escalation.

C1 Enhancement: Through Professional Services, C1 helps deploy and integrate Palo Alto's Prisma Access and Cortex XDR, delivering a unified threat view and eliminating blind spots.

☐ Yes ☐ No ☐ Not sure

3 Behavior-Based Threat Detection and Precision AI™

What it is: Behavior-based detection uses machine learning to identify anomalies or suspicious patterns rather than relying only on known signatures or rules. Palo Alto's Precision AI™ continuously learns from billions of threat indicators across its ecosystem.

Why it matters: Modern attackers use polymorphic malware, fileless attacks, and "living off the land" techniques that bypass traditional detection. Behavior-based analysis catches what static tools miss.

C1 Enhancement: C1 Advisory Services work with your team to align detection policies with your unique threat profile, and C1's Managed Services monitors the threat models across your business.

☐ Yes ☐ No ☐ Not sure

4 Automated Playbooks and Response Orchestration

What it is: Playbooks are sequences of automated actions triggered by specific threat events. These can isolate infected devices, revoke credentials, block IPs, or notify stakeholders, without waiting for human intervention.

Why it matters: Time is everything in threat response. Orchestration tools like SOAR reduce dwell time and limit the damage by responding instantly and consistently.

C1 Enhancement: C1's Professional Services team can design and implement Palo Alto Networks SOAR playbooks that automate threat response actions like device isolation, credential revocation, and stakeholder notification. While C1 does not provide Managed Services for Palo Alto's SOAR platform, our experts can help operationalize automation strategies that accelerate containment and reduce manual workloads.

☐ Yes ☐ No ☐ Not sure

5 Zero Trust Enforcement and Identity-Aware Access

What it is: Zero Trust means no user or device is trusted by default, even inside the network. Palo Alto's ZTNA 2.0 enforces this by requiring continuous authentication, assessing device posture, and segmenting access by policy.

Why it matters: 81% of breaches involve compromised credentials. Zero Trust prevents lateral movement even when an attacker gains initial access.

C1 Enhancement: C1 Advisory Services help define your Zero Trust architecture, while our Professional Services implement ZTNA controls across your cloud, users, and apps.

☐ Yes ☐ No ☐ Not sure

Scoring: What Your Answers Reveal

Score	What It Means	Customer Profile
5 Yes Answers	You've built a strong foundation for AI-powered defense.	You're a forward-thinking enterprise with mature security ops, already leveraging automation and unified visibility. C1 can help you fine-tune, scale, or expand your strategy.
3–4 Yes Answers	You're on the path, but critical gaps remain.	You likely have strong components in place (EDR, SIEM, cloud monitoring), but need help integrating systems or operationalizing AI-driven workflows. C1's phased support model is ideal.
0–2 Yes Answers	You're highly vulnerable to today's threats.	You may be relying on manual alerts, fragmented tools, or aging firewalls. It's time to modernize before a breach occurs. C1 can guide your transition with minimal disruption.

Why C1 + Palo Alto Are Built for Modern Threat Defense

Palo Alto Networks delivers the technology. C1 delivers the outcome.

Together, they provide a seamless combination of cutting-edge AI-driven security platforms and the human expertise needed to design, deploy, and run them effectively.

Palo Alto Networks brings:

Precision AI™ for accurate, automated detection and response

Cortex XDR/XSIAM for full-spectrum visibility across hybrid environments

Prisma Access for secure connectivity across users, apps, and cloud

ZTNA 2.0 to enforce granular, identity-aware access controls

C1 brings:

Advisory Services to align your security strategy with risk and compliance goals

Professional Services to design and deploy Palo Alto tools to fit your architecture

Managed Services to monitor, manage, and continuously optimize your defenses, 24/7

Bottom Line:

Most vendors offer products. C1 offers a security journey. Whether you're building a Zero Trust program, automating threat response, or unifying multi-cloud visibility, C1 helps you get there faster, with less risk and more value.

Ready to modernize your threat protection?

Get started with a C1 expert today: www.onec1.com/what-we-do/security